"A Brief Review on Different security mechanism in cloud Computing"

Miss. Suvidha S. Sangole[1], Asst.Prof. M.R. Ingle [2], Asst.Prof. Sangharsh B. Lanjewar[3]

[1] PG Student ,Departement of computer science and engg,
DBACER, Nagpur, India.
ss.suvidha01@gmail.com

[2] Departement of computer science and engg,
DBACER, Nagpur, India.
mitali_mits2007@rediffmail.com

[3] Departement of computer science and engg,
DBACER, Nagpur, India.
langewar.sangharsh@gmail.com

***Abstract*—** A new approach which comes from grid computing, distributed computing, parallel computing, virtualization technology is namely known as cloud computing technology. Due to advantage of low cost and ease of access cloud computing has get popularity. But ensuring the security of cloud computing is a major goal in the cloud computing environment. In this paper, we are proposing a simple, effective, and broadly verifiable approach to ensure cloud data integrity and reliability without sacrificing the inscrutability of data owners. The previous security system only concentrates on the authentication; it only focused on the user private and sensitive important data is not accessed by unauthorized user. To mention above cloud security as well as privacy issue we are going to use (SAPA) Shared authority based privacy preserving authentication protocol. The proposed SAPA technology is achieved anonymous access request and privacy consideration, attribute based access control allows the single user to access his own data. Proxy re-encryption scheme is used by cloud server for accessing data from the other trusted party and sharing among multiple users. It specifies that the proposed scenario is probably applied for enriched privacy-preservation and security in cloud applications.

Keyword: Authentication protocols, SAPA, Cloud computing, Cloud computing security, Data security.

I. INTRODUCTION

Cloud computing is one of the emerging and rapidly growing technologies. The cloud environment is distributed system which is a large open environment which is 24/7 available online. Hence it is essential to sheltered sensitive data of user as well as provides privacy of user, without manner in mind the local infrastructure restrictions; the cloud services allow the user to enjoy the cloud applications functionality. For example in the cloud storage based supply chain management here are various interest groups (e.g., supplier, carrier, and retailer) in the system. Each group holds its users, then that users have given authorization to access the authorized data fields, and different users own moderately autonomous access authorities. It means that any two users from a variety of groups should access different data fields of the same file. For example, a supplier consciously may want to access a carrier's data fields, but it is not confident whether the carrier will allow its access request. If the carrier denied its access request, the supplier's access need will be exposed along with nothing obtained towards the preferred data fields. Basically, the supplier may not send the access request or extract the un-accepted request in growth if it unquestionably knows that its request will be denied by the carrier. It is bad-tempered to thoroughly disclose the supplier's private information without any privacy concerns.

There are subsequent three issues are arises from above example:

• The carrier also desires to access the supplier's data fields, and the cloud server should inform each other and broadcast the shared access authority to the both users.

• The carrier has no significance on other users' data fields, therefore its approved data fields should be suitably protected, and meanwhile the supplier's access request will also be secreted.

• The carrier may need to access the retailer's data fields, but it is not certain whether the retailer will receive its request or not. The retailer's certified data fields should not be public if the retailer has no interests in the carrier's data fields, and the carrier's request is also surreptitiously hidden.

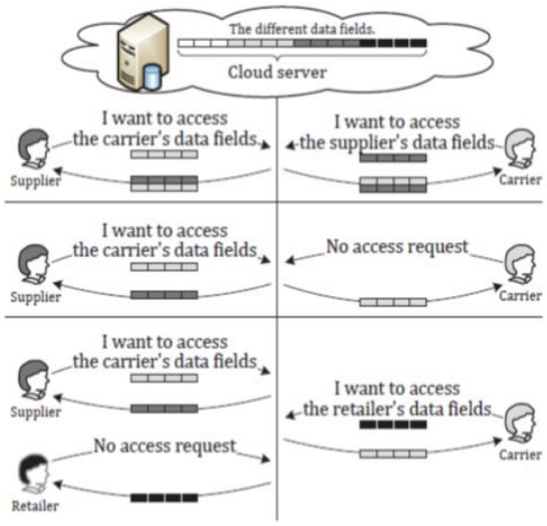

Fig. 1. Three possible cases during data accessing and data sharing in cloud applications.

Towards above three cases, security defences and privacy preservation are both considered without illuminating sensitive access need related information.

In the cloud environment, a reasonable security protocol should accomplish the following requirements:

1) Authentication: An authorized user can access its own data fields, only the approved incomplete or entire data fields can be predictable by the legal user, and any fictitious or tampered data fields cannot cheat the legal user.

2) Data anonymity: Any improper entity cannot categorize the proxy data and communication state even it intercepts the exchanged messages via an open channel.

3) User privacy: Any improper unit cannot know or guess a user's access needs, which indicate a user's concern in another user's authorized data fields. If and only if the both users have common interests in each other's authorized data fields, the cloud server will report to the two users to understand the access permission sharing.

4) Forward security: Any challenger cannot associate two communication terms to obtain the prior interrogations according to the currently captured messages.

We discussion the above-mentioned privacy issue to intend a shared authority based privacy preserving authentication protocol (SAPA) for the cloud data storage, which realizes authentication and authorization without sacrificing a user's private and legal as well as sensitive information.

The following are the contributions:

1) Recognize a new privacy dispute in cloud storage, and address a restrained privacy issue during a user testing the cloud server for data sharing, in which the challenged request itself cannot expose the user's privacy no matter whether or not it can acquire the access right.

2) Recommend an authentication protocol to improve a user's access request related privacy, and the shared access authority is achieved by anonymous access request similar mechanism.

3) Apply cipher text-policy attribute based access control to appreciate that a user can consistently access its own data fields, and espouse the proxy re-encryption to provide temp authorized data sharing among multiple users.

II. EXISTING APPROACH

Deyan Chen, Hong Zhao [2] they have provides a short but multitalented analysis on data security and privacy protection issues associated with cloud computing across all segments of data life cycle. They have discussed some in progress solutions. Finally, they have describes future research work about data security and privacy protection issues in cloud computing environment.

Ramgovind S, Eloff MM, Smith E [3] they have provide an generally security observation of Cloud computing with the purpose to emphasize the security uncertainties that should be correctly addressed and managed to appreciate the full possible of cloud computing.

Chia-Mu Yu, Chi-Yuan Chen, and Han-Chieh Chao [1] they had aiming to reducing both the server side dormancy and the user side dormancy, they had projected an substitute POW design on the problem of unauthorized file downloading in de-duplicated cloud storage. Since the Bloom filter has been used extensively in various applications and is easy to be implemented, there projected POW scheme is considered reasonable and can be organized in real-world cloud storage facilities.

H. Wang **[5]** have study proxy provable data possession (PPDP). In public clouds, PPDP is a matter of essential significance when the client cannot execute the remote data possession inspection. He had study the PPDP system structure, the security model, and the design technique. Based on the bilinear pairing technique, he had design a resourceful PPDP protocol. Through security examination and performance examination, our protocol is provable secure and efficient.

P. Vidhya Lakshmi,Dr. S. Sankar Ganesh [4] they had acknowledged a new privacy challenge during data accessing. Data discretion and data reliability is assured by authentication. During the broadcast the covered values are exchanged hence data anonymity is accomplished. Anonymous access requests raise the user privacy that

confidentially informs the cloud server about the user access requirements. To prevent the assembly correlation, the assembly identifiers realizes the forward security. They had projected scheme can useful for improved privacy preservation in cloud applications.

Somesh P. Badhel, Prof. Vikrant Chole [7] had provide the review on all the techniques and tried to cover different challenges of data backup and recovery of data after scratch for Cloud Computing such as maintaining the cost of execution and accomplishment complexities as low as possible. However each one of the backup procedure solution for Cloud Computing is not competent to accomplish all the challenges of remote data back-up server with less minimum storage space.

Somesh P. Badhel, Prof. Vikrant Chole [8] had projected attribute design of proposed Backup recovery technique for cloud computing. There projected procedure is strong in serving the users to congregate information or data from any remote location in the lack of network connectivity and also to progress the files in case of the file deletion or if the cloud gets crushed due to any reason also it reduces the memory requirement of backup cloud to a lower value as compared to main cloud, this achieves advanced competence as compared to previous backup technologies for cloud computing. They had shown that projected method also focuses on the security perception for the back-up files stored at remote server, without using any of the preceding encryption techniques. There proposed technique also solves time associated issues that will take less time for recuperation process as compare to other.

Apurva Gomase, Prof.Vikrant Chole [6] had projected re-encryption in which the data is encrypting twofold. So this method is proficient and scalable to securely handle users private and perceptive data in the data sharing system user ensures about the data storage in exterior data storing center. Data privacy and discretion in the data sharing system in opposition to any system managers or user as well as adversarial outsiders without corresponding recommendation. Instantaneous user revocation result to manage the system professionally from unauthorized user to access authorized user data.

III. PROBLEM FORMULATION

The Main intention is to put into practice a shared authority based privacy-preserving authentication protocol to tackle above privacy issue for cloud storage.
For Achieving the Above purpose we are proposing:

- Shared access authority is achieved by unidentified access request corresponding mechanism with security and privacy considerations (e.g., authentication, data anonymity, user privacy, and forward security);
- Attribute based access control is adopted to understand that the user can only access its own data fields;
- Proxy re-encryption is functioned by the cloud server to provide data sharing among the multiple users.

IV. PROPOSED METHOD

We have documented privacy disputes during data accessing and sharing in the cloud computing surroundings. Classify a new privacy assignment in cloud storage, and address a circuitous privacy issue during a user interesting the cloud server for data sharing and data accessing, in which the challenged request itself cannot make known the user's privacy no matter whether or not it can get your hands on the access authority.

We have projected an authentication protocol to amplify a user's access request connected privacy, and the shared access authority is achieved by unidentified access request similar mechanism.

Apply cipher text-policy attribute based access control to appreciate that a user can consistently access its own data fields, and recognize the proxy re-encryption to provide temp authorized data sharing among numerous users.

The most important goal is to execute a shared authority based privacy-preserving authentication protocol (SAPA) to discourse above privacy concern for cloud storage. For targeting the above goal we have projected a Shared access authority is achieved by unidentified access request similar mechanism with security and privacy concerns (e.g., authentication, data anonymity, user privacy, and forward security);

Attribute based access control is acknowledged to appreciate that the user can only access its own data fields; Proxy re-encryption is applied by the cloud server to provide data sharing among the multiple users.

V. CONCLUSIONS

In this paper, we have proposed a privacy preserving access authority sharing in cloud computing environment. Where we will acknowledged a new privacy assignment during data accessing. Data discretion and data reliability will be distinct by authentication. During the broadcast the wrapped values will be exchanged hence data anonymity will be achieved. User privacy is improved by unidentified access request to confidentially notify the cloud server about the

user's access necessitate. We have proposed a shared access authority by unidentified access request corresponding mechanism with security and privacy considerations , attribute based access control will help to appreciate that the user can only access its own data fields; proxy re-encryption by the cloud server will provide data sharing among the numerous users. This shows that the proposed scheme can applied for improved privacy preservation in cloud application.

VI. REFERENCES

[1] Deyan chen, hong zhao, "Data security and privacy protection issue in cloud computing"IEEE conference of computer science and electronics engg, 2013.

[2] Ramgovind S, Eloff MM, Smith E,"The management of security in cloud computing".

[3] Chia-Mu Yu, Chi –Yuan Chen, Han-Chieh Chao,"proof of ownership in de-duplicated cloud storage with mobile efficiency".

[4] Wang, "Proxy Provable Data Possession in Public Clouds,"IEEE Transactions on Services Computing, [online]ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6357181, 2012.

[5] Somesh P. Badhel, Vikrant Chole, "A review on data back-up techniques for cloud computing", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.12, December-2014, pg. 538-542.

[6] Somesh P. Badhel, Prof. Vikrant Chole, "An efficient and secure remote data back-up technique for cloud computing", International Journal of Computer Science and Mobile Computing, Vol.4 Issue.6, June- 2015, pg. 361-36

[7] Apurva Gomase, Prof.Vikrant Chole, "Secure system implementation using attribute based encryption", ijates,Vol.No.03,Special issue No.01,Nov 2015

[8] L. A. Dunning and R. Kresman, "Privacy Preserving Data Sharing With Anonymous ID Assignment," IEEE Transactions on Information Forensics and Security, *vol. 8, no. 2, pp. 402-413, 2013.* X. Liu, Y. Zhang, B. Wang, and J. Yan.

[9] Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Transactions on Parallel and Distributed Systems, [online] ieeexplore. ieee.org/stamp/stamp.jsp?tp=&arnumber=6374615, 2012.

[10] S. Grzonkowski and P. M. Corcoran, "Sharing Cloud Services: User Authentication for Social Enhancement of Home Networking,"IEEE Transactions on Consumer Electronics, vol. 57, no. 3, pp.1424-1432, 2011.

[11] M. Nabeel, N. Shang and E. Bertino, "Privacy Preserving Policy Based Content Sharing in Public Clouds," IEEE Transactions on Knowledge and Data Engineering, [online] ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6298891, 2012.

[12] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Transactions on Services Computing, vol. 5, no. 2, pp. 220-232, 2012.

[13] S. Sundareswaran, A. C. Squicciarini, and D. Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud," IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 4, pp. 556-568, 2012.

[14] J. Chen, Y. Wang, and X. Wang, "On-Demand Security Architecture for Cloud Computing," Computer, vol. 45,no. 7, pp. 73-78,2012.

[15] Y. Zhu, H. Hu, G. Ahn, and M. Yu, "Cooperative Provable Data Possession for Integrity Verification in Multi-cloud Storage",IEEE Transactions on Parallel and Distributed Systems, vol. 23, no, 12, pp. 2231-2244, 2012.